Код документа ДИБ-ПЛ-02
Зарегистрировано в
Журнале регистрации внутренних нормативных
документов юридического департамента
АО «Инвестиционный Дом «Астана-Инвест»
от «29» сентября 2023 г. за № 400

Редакция № 1

УТВЕРЖДЕНА
Советом директоров
АО «Инвестиционный Дом «Астана-Инвест»
протокол № 8 от «29» 09 2023 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «Инвестиционный Дом «Астана-Инвест»

Оглавление

Глава 1. Общие положения

1. АО «Инвестиционный Дом «Астана-Инвест» (далее – Компания) отдельно выделяет вопросы обеспечения информационной безопасности, непрерывно совершенствует систему менеджмента информационной безопасностью (далее – СМИБ), а также занимается развитием применяемых средств и способов защиты от угроз кибербезопасности и обеспечивает необходимые компетенции работников в области защиты информации.
2. Политика информационной безопасности (далее - Политика) базируется на требованиях стандарта СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования» и предназначена для публикации на корпоративном веб-сайте Компании с целью демонстрации приверженности в вопросах обеспечения кибербезопасности и поддержки со стороны руководства Компании.
3. Нормативно-правовую основу Политики составляют положения законодательства Республики Казахстан по вопросам использования информационных систем и информационной безопасности, а также требования международных стандартов управления информационной безопасностью.
4. Положения Политики обязательны для исполнения всеми работниками Компании, а также должны доводиться до сведения клиентов и иных третьих лиц, имеющих доступ к информационным системам и документам Компании, в той их части, которая непосредственно взаимосвязана с Компанией и их деятельностью.
5. Политика охватывает все информационно-коммуникационные системы и данные, владельцем и пользователем которых является Компания. Обеспечение информационной безопасности – одно из важнейших условий для успешного осуществления деятельности Компании.

Глава 2. Цель

6. Основной целью, на которую направлены все положения Политики, является минимизация ущерба от событий, несущих угрозу безопасности информации, посредством их предотвращения или минимизации последствий от их наступления.
7. Обеспечение информационной безопасности Компании необходимо для снижения рисков, финансового ущерба и репутационных потерь, связанных со всевозможными угрозами в отношении информационных ресурсов Компании.
8. С этой целью Компания непрерывно поддерживает главные свойства информации, а именно:
   1) доступность – свойство информации, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия;
   2) конфиденциальность – свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;

3) целостность – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к эталонному/фиксированному ее состоянию).

9. Защита объектов информатизации Компании осуществляется в соответствии с законодательством Республики Казахстан и действующими на территории Республики Казахстан стандартами в целях обеспечения целостности, сохранности, обеспечения режима конфиденциальности и реализации права на доступ к информационным ресурсам, а также в целях недопущения нарушений функционирования объектов информационно-коммуникационной инфраструктуры и недопущения несанкционированных и (или) непреднамеренных действий (доступ, блокирование, модификация, копирование, уничтожение) в отношении объектов обеспечения информационной безопасности.
10. Процесс создания надежной защиты информации является непрерывным. В целях обеспечения достаточно надежной СМИБ необходима постоянная регулировка ее параметров, адаптация для противодействия новым внешним и внутренним угрозам.

Глава 3. Основные принципы построения СМИБ

11. Построение СМИБ Компании и ее функционирование должны осуществляться в соответствии со следующими основными принципами:
    1) законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Компании;
    2) ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки основной деятельности. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности Компании;
    3) непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Компании должны осуществляться без прерывания или остановки текущих бизнес-процессов Компании;
    4) комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;
    5) применимость и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем информационной безопасности должна быть меньше размера потенциального ущерба от любых видов угроз.

Глава 4. Объекты обеспечения информационной безопасности и виды защищаемой информации

12. Основными объектами обеспечения информационной безопасности Компании определены следующие элементы:
    1) информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Компании к коммерческой тайне Компании, а также сведения, содержащие персональные данные клиентов и работников Компании;
    2) средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;
    3) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы Компании, с помощью которых производится обработка защищаемой информации;
    4) процессы Компании, связанные с управлением и использованием информационных ресурсов;
    5) помещения, в которых расположены средства обработки защищаемой информации;
    6) рабочие помещения и кабинеты работников Компании, а также помещения Компании, предназначенные для ведения закрытых переговоров и совещаний;
    7) работники Компании, имеющие доступ к защищаемой информации;
    8) технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.
13. Защищаемая информация определяется как имеющая материальный носитель, так и электронный (цифровой) вид.
14. Защищаемая информация может размещаться на бумажных и иных носителях, обладающих свойствами ее визуального воспроизведения в виде надписей, оттисков, копий и отражений;
15. Защищаемая информация в электронном виде обрабатывается, передается и хранится посредством вычислительной техники, может записываться и воспроизводиться с помощью различных технических средств.
16. Защищаемая информация может передаваться по телефону в виде электрических сигналов.

Глава 5. Угрозы информационной безопасности

17. Под угрозами информационной безопасности понимается потенциальная возможность нарушения главных свойств информации – конфиденциальности, целостности и доступности.
18. К числу угроз информационной безопасности относятся (но не ограничены ими):
    1) утрата информации, составляющих коммерческую тайну Компании и иную защищаемую информацию;
    2) искажение (несанкционированная модификация, подделка) защищаемой информации;

3) утечка информации – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.);
4) несанкционированное использование информационных ресурсов (злоупотребления, мошенничества и т.п.);
5) недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, активного сетевого оборудования, систем управления базами данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств и злонамеренных действий.

Глава 6. Классификация нарушителей информационной безопасности

19. Нарушители информационной безопасности классифицируются следующим образом:
    1) внутренние нарушители – работники Компании, неосознанно либо злонамеренно нарушающие режим информационной безопасности;
    2) внешние нарушители – лица, не связанные с Компанией трудовыми отношениями (в том числе стажеры и практиканты), из хулиганских или корыстных побуждений предпринимающие действия, способные нанести ущерб информационным ресурсам Компании.
20. Опасность нарушителя определяется количеством и степенью важности доступных ему информационных ресурсов и уровнем полномочий в Компании.
21. Исходя из этого, наиболее рисковыми категориями следует считать менеджеров высшего и среднего звена, администраторов информационных ресурсов и лиц, работающих с большими объемами клиентской и финансовой информации.

Глава 7. Классификация видов ущерба при реализации угроз информационной безопасности

22. В результате воздействия угроз информационной безопасности, могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности Компании и ее нормальное функционирование:
    1) финансовые потери, связанные с утечкой или разглашением защищаемой информации;
    2) финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
    3) ущерб от дезорганизации деятельности Компании и потери, связанные с невозможностью выполнения им своих обязательств;
    4) ущерб от принятия управленческих решений на основе необъективной информации;
    5) ущерб от отсутствия у руководства Компании объективной информации для принятия решений;
    6) ущерб, нанесенный репутации Компании и иной вид ущерба.

Глава 8. Меры по обеспечению информационной безопасности

23. Основными мерами по обеспечению информационной безопасности Компании, направленными на сохранность объектов информатизации, предотвращения неправомерного и (или) непреднамеренного доступа и (или) воздействия на них, являются:
    1) административно-правовые и организационные меры;
    2) меры физической безопасности;
    3) программно-технические меры.
24. Административно-правовые и организационные меры включают (но не ограничиваются):
    1) контроль исполнения требований законодательства РК и внутренних документов Компании;
    2) контроль соответствия бизнес-процессов требованиям Политики;
    3) реагирование на инциденты, локализацию и минимизацию последствий;
    4) анализ новых рисков информационной безопасности;
    5) отслеживание и улучшение морально-делового климата в коллективе;
    6) определение действий при возникновении чрезвычайных ситуаций;
    7) проведение профилактических мер при приеме на работу и увольнении работников Компании;
    8) информирование и обучение работников Компании работе с информационными системами и требованиям информационной безопасности;
    9) разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику.
25. Меры физической безопасности включают (но не ограничиваются):
    1) организацию пропускного и внутриобъектового режимов;
    2) построение периметра безопасности защищаемых объектов;
    3) организацию противопожарной безопасности охраняемых объектов;
    4) контроль доступа работников Компании в помещения ограниченного доступа;
    5) организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности.
26. Программно-технические меры включают (но не ограничиваются):
    1) использование лицензионного программного обеспечения и средств защиты информации;
    2) использование средств защиты периметра;
    3) применение комплексной антивирусной защиты;
    4) использование средств информационной безопасности, встроенных в информационные системы;
    5) обеспечение регулярного резервного копирования информации;
    6) контроль за правами и действиями пользователей, в первую очередь, привилегированных;
    7) применение средств криптографической защиты информации;
    8) обеспечение безотказной работы аппаратных средств;
    9) мониторинг состояния критичных элементов информационной системы.

Глава 9. Регуляторные требования и Compliance

27. Настоящая Политика и система информационной безопасности в целом опираются на нормативные правовые акты, международные и национальные стандарты, напрямую влияющие на процесс функционирования СМИБ Компании. В то же время, существует ряд документов, который либо описывает стратегические аспекты развития информационной безопасности на государственном уровне, либо регламентирует правила по информационной защите отдельных приложений и услуг:
    1) Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан»;
    2) Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")»;
    3) Закон Республики Казахстан от 2 июля 2003 года № 461 «О рынке ценных бумаг»;
    4) Закон Республики Казахстан от 21 мая 2013 года N 94-V «О персональных данных и их защите»;
    5) Закон Республики Казахстан от 7 января 2003 года № 370 «Об электронном документе и электронной цифровой подписи»;
    6) Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации»;
    7) Постановление Правления Национального Банка Республики Казахстан от 28 апреля 2012 года № 165 «Об утверждении Требований к программно-техническим средствам и иному оборудованию, необходимым для осуществления деятельности на рынке ценных бумаг»;
    8) Постановление Правления Национального Банка Республики Казахстан от 27 августа 2013 года № 214 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для организаций, осуществляющих брокерскую и дилерскую деятельность на рынке ценных бумаг, деятельность по управлению инвестиционным портфелем»;
    9) Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 23 ноября 2020 года № 110 «Об утверждении Правил оценки уровня защищенности от угроз информационной безопасности»;
    10) Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 23 ноября 2020 года № 111 «Об утверждении методики оценки рисков информационной безопасности, включая порядок ранжирования финансовых организаций по степени подверженности рискам информационной безопасности»;
    11) Постановление Правления Национального Банка Республики Казахстан от 3 февраля 2014 года № 9 «Об утверждении Правил осуществления брокерской и (или) дилерской деятельности на рынке ценных бумаг, порядка проведения брокером и (или) дилером банковских операций».

Глава 10. Пересмотр Политики информационной безопасности

28. Пересмотр положений настоящей Политики осуществляется Департаментом информационной безопасности Компании, и включает оценку возможности улучшения ее положений и процесса управления информационной безопасностью в соответствии с изменениями.
29. Плановый пересмотр положений настоящей Политики осуществляется не реже одного раза в три года.
30. Внеплановый пересмотр Политики проводится в случае:
    1) внесения существенных изменений в Устав и организационную структуру Компании;
    2) значимых изменений в законодательстве, регулирующих основную деятельность Компании;
    3) возникновения значимых инцидентов информационной безопасности;
    4) изменения бизнес-процессов Компании.
31. При внесении изменений в результате пересмотра Политики учитываются:
    1) результаты аудита информационной безопасности, а также результаты предыдущих аудитов;
    2) рекомендации независимых экспертов по информационной безопасности;
    3) существенные угрозы и уязвимости информационной системы;
    4) отчеты об инцидентах в области информационной безопасности;
    5) рекомендации органов государственной власти.

Председатель Правления **Маеплаева И.Я.**